

(iii) Maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and commingled with training records of other students (for example, admission forms, transcripts, academic counseling and similar records).

(iv) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with the Federal Claims Collection Act of 1966, 31 U.S.C. 3711(e).

(v) Maintained by the contractor incident to normal business practices and operations.

(4) The DoD Components shall publish instructions that:

(i) Furnish DoD Privacy Program guidance to their personnel who solicit, award, or administer Government contracts;

(ii) Inform prospective contractors of their responsibilities, and provide training as appropriate, regarding the DoD Privacy Program; and

(iii) Establish an internal system of contractor performance review to ensure compliance with the DoD Privacy Program.

(b) *Contracting procedures.* The Defense Acquisition Regulations Council shall develop the specific policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to this part.

(c) *Contractor compliance.* Through the various contract surveillance programs, ensure contractors comply with the procedures established in accordance with § 310.12(b).

(d) *Disclosure of records to contractors.* Disclosure of records contained in a system of records by a DoD Component to a contractor for use in the performance of a DoD contract is considered a disclosure within the Department of Defense (see § 310.21(b)). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

§ 310.13 Safeguarding personal information.

(a) *General responsibilities.* DoD Components shall establish appropriate ad-

ministrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

(b) *Minimum standards.* (1) Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

(2) Treat all unclassified records that contain personal information that normally would be withheld from the public under Freedom of Information Exemption Numbers 6 and 7 of 286.12, subpart C of 32 CFR part 286 (“DoD Freedom of Information Act Program”) as “For Official Use Only,” and safeguard them accordingly, in accordance with DoD 5200.1-R even if they are not actually marked “For Official Use Only.”

(3) Personal information that does not meet the criteria discussed in paragraph (b)(2) of this section shall be accorded protection commensurate with the nature and type of information involved.

(4) Special administrative, physical, and technical procedures are required to protect data that is stored or processed in an information technology system to protect against threats unique to an automated environment (see appendix A).

(5) Tailor safeguards specifically to the vulnerabilities of the system.

(c) *Records disposal.* (1) Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods are those approved by the Component or the National Institute of Standards and Technology. For paper records, disposal methods, such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, or mutilation are acceptable. For electronic records, and media, disposal methods, such as overwriting, degaussing, disintegration,

Office of the Secretary of Defense

§ 310.14

pulverization, burning, melting, incineration, shredding or sanding, are acceptable.

(2) Disposal methods are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

§ 310.14 Notification when information is lost, stolen, or compromised.

(a) If records containing personal information are lost, stolen, or compromised, the potential exists that the records may be used for unlawful purposes, such as identity theft, fraud, stalking, etc. The personal impact on the affected individual may be severe if the records are misused. To assist the individual, the Component shall promptly notify the individual of any loss, theft, or compromise (See also, § 310.50 for reporting of the breach to Senior Component Official for Privacy and the Defense Privacy Office).

(1) The notification shall be made whenever a breach occurs that involves personal information pertaining to a service member, civilian employee (appropriated or non-appropriated fund), military retiree, family member, DoD contractor, other persons that are affiliated with the Component (e.g., volunteer), and/or any other member of the public on whom information is maintained by the Component or by a contractor on behalf of the Component.

(2) The notification shall be made as soon as possible, but not later than 10 working days after the loss, theft, or compromise is discovered and the identities of the individuals ascertained.

(i) The 10 day period begins to run after the Component is able to determine the identities of the individuals whose records were lost.

(ii) If the Component is only able to identify some but not all of the affected individuals, notification shall be given to those that can be identified with follow-up notifications made to those subsequently identified.

(iii) If the Component cannot readily identify the affected individuals or will not be able to identify the individuals, the Component shall provide a generalized notice to the potentially impacted population by whatever means the Component believes is most likely to reach the affected individuals.

(3) When personal information is maintained by a DoD contractor on behalf of the Component, the contractor shall notify the Component immediately upon discovery that a loss, theft or compromise has occurred.

(i) The Component shall determine whether the Component or the contractor shall make the required notification.

(ii) If the contractor is to notify the impacted population, it shall submit the notification letters to the Component for review and approval. The Component shall coordinate with the Contractor to ensure the letters meet the requirements of § 310.14.

(4) Subject to paragraph (a)(2) of this section, the Component shall inform the Deputy Secretary of Defense of the reasons why notice was not provided to the individuals or the affected population within the 10-day period.

(i) If for good cause (e.g., law enforcement authorities request delayed notification as immediate notification will jeopardize investigative efforts), notice can be delayed, but the delay shall only be for a reasonable period of time. In determining what constitutes a reasonable period of delay, the potential harm to the individual must be weighed against the necessity for delayed notification.

(ii) The required notification shall be prepared and forwarded to the Senior Component Official for Privacy who shall forward it to the Defense Privacy Office. The Defense Privacy Office, in coordination with the Office of the Under Secretary of Defense for Personnel and Readiness, shall forward the notice to the Deputy Secretary.

(5) The notice to the individual, at a minimum, shall include the following:

(i) The individuals shall be advised of what specific data was involved. It is insufficient to simply state that personal information has been lost. Where names, social security numbers, and dates of birth are involved, it is critical that the individual be advised that these data elements potentially have been compromised.

(ii) The individual shall be informed of the facts and circumstances surrounding the loss, theft, or compromise. The description of the loss should be sufficiently detailed so that